

Original Research Article

Research on Payment Security under the Integration of New Media and E-Commerce

Yushui Xiao*, Yujie Li, Yong Huang

SEGi University, Kuala Lumpur, 47810 Malaysia. E-mail: 957188080@qq.com

Abstract: With the popularization and development of the network, e-commerce is gradually integrated into the daily life of people, thus effectively promoting the transformation of the traditional production and living mode in China. As the core content, online payment is the foundation to ensure the smooth development of e-commerce. At the present stage, there are still some deficiencies, which has had a negative impact on the security of China's online payment. This paper analyzes and explores the security problems in the current online payment process of China, and puts forward targeted countermeasures to lay a foundation for the improvement of e-commerce security.

Keywords: Online Payment; E-Commerce; Property Safety; Targeted Countermeasures

In recent years, with the continuous development of network technology, e-commerce has become one of the important contents in people's social life. Relevant research shows that in recent years, with the emergence and vigorous development of well-known e-commerce enterprises such as Taobao, JD and Pinduoduo, e-commerce has achieved a great progress in China. In the process of e-commerce, as one of the bases of trading activities, online payment is the determining factor of the smooth development of e-commerce. Therefore, people pay more and more attention to payment security issues. In order to further ensure the payment security of users, according to the researchers, relevant enterprises and departments should actively explore the payment security issues so as to promote the continuous optimization of online payment security.

1. Status quo of the development of online payment in China

As the core content of e-commerce, online payment has shown strong development potential along with the development of e-commerce. According to incomplete statistics, by 2019, China's online shopping users exceeded 600 million, while the total annual e-commerce transactions reached 34.81 trillion yuan, which indicates that online payment in China has developed rapidly. In the developing process of online payment, payment security has gained more attention from network users with the occurrence of security incidents. Therefore, actively ensuring the security of online payment is of positive value for promoting its healthy development.

2. Security problems of e-commerce in the payment process

2.1 Low network security and various types of network fraud

In the process of online payment, some criminals often counterfeit well-known websites through counterfeiting URL addresses, then induce network users to log in their accounts and passwords in fake websites, thus stealing users'

Copyright © 2020 Yushui Xiao *et al.*

doi: 10.18282/ff.v9i1.807

This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

passwords. At the same time, relevant personnel can detect the terminal payment process of users through tracking software, thus realizing the purpose of stealing users' account number and password and further damaging the security of users' funds in the account.

2.2 Insufficient performance of system security to deal with hackers and virus attacks

Due to the lack of system security performance, malicious attacks by hackers impact greatly on system security. As for the attack mode, attacker mainly control and detect the users' system by writing program codes, thus stealing information. In this process, most hackers realize the mastery of users' information through Trojan implantation in the system, which is relatively hidden and often difficult for users to detect. In addition, some hackers can also release and spread viruses by inserting malicious codes into web pages, thereby causing damage to the system.

2.3 Insufficient information security increasing the security risks in the payment process

In the process of online payment, information security issues have a serious impact on users' payment security. Generally speaking, information security problems mainly include three types, namely information disclosure, impersonation of legitimate users and malicious information tampering. The main content of the information security problem is that criminals can steal the user's information in order to impersonate the user's identity, further causing damage to the user's account. At the same time, the existence of information problems, to a certain extent, leads to a serious impact on users' information security, which is not conducive to the reasonable protection of privacy.

2.4 The lack of supervision system hindering the implementation of network supervision work

From the perspective of supervision, at this stage, China has not yet effectively established and perfected the supervision mechanism on the issue of e-commerce, which is not conducive to the effective protection of the legitimate rights and interests of users. In addition, due to the lack of supervision system, it is often difficult for users to effectively and reasonably protect their rights and interests, restricting the reasonable establishment of users' confidence in online payment, and causing serious impact on the security of online payment.

3. Countermeasures of online payment security issues

3.1 Raise the communication access threshold and strengthen network security management

In order to effectively improve the quality of network security, relevant departments should actively improve the network environment in a reasonable way so as to effectively optimize the network environment and the management effect. In terms of specific measures, on the one hand, enterprises should actively and rationally apply advanced technologies in order to reasonably block viruses. At the same time, in order to effectively monitor malicious websites, relevant departments should actively strengthen the firewall technology in order to successfully avoid the influence of malicious network information. In addition, in order to further realize the effective control of bad websites, relevant departments should actively improve the communication access threshold and strengthen the management ability for website construction, so as to maximize the improvement of network security level.

3.2 Optimize the system performance and improve the attack resistance

Regarding to the issue of system performance, researchers pointed out that enterprises should actively optimize the system performance in order to further enhance the system's ability to resist hacker attacks, thus laying a foundation for the promotion and optimization of payment security products. On this issue, first of all, relevant departments should effectively carry out reasonable optimization of system capabilities in order to enhance their ability to resist different types of viruses and Trojan, and better deal with the threats brought by hacker attacks. On the other hand, relevant departments should treat hackers and other network attackers seriously and effectively carry out ideological education work, so as to help them change their ideas to effectively apply network technology capabilities to contribute to social development, avoid them from continuing to attack network system, and thus reasonably optimize network system

security.

3.3 Implement construction of credit system and reasonably protect information security

In order to effectively guarantee information security, the social credit system should be actively constructed and perfected in China, so as to guarantee e-commerce security. In this process, relevant departments should actively establish and perfect credit records for major dishonest people, so as to strengthen the network management, effectively prevent network technology crimes and lay a good foundation and guarantee for the improvement of China's online payment management level. For example, through constructing information base of dishonest people, in the process of e-commerce, it is beneficial for users and merchants to strengthen prevention awareness of payment risk, thus avoiding the occurrence of payment risks.

3.4 Improve the management system and strengthen network supervision

Regarding to the problem of insufficient supervision for online payment, relevant departments and e-commerce enterprises should actively carry out communication and cooperation, so as to promote the establishment and improvement of e-commerce management laws and regulations, and further standardize e-commerce transactions. Meanwhile, in the daily work, the relevant departments should actively carry out propaganda of security knowledge of e-commerce payment, in order to enhance people's awareness of online payment security, thus laying the foundation and guarantee for strengthening management effect of online payment.

4. Conclusion

In general, with the continuous popularization and development of network technology, e-commerce has become one of the main trends in the current social development. In this process, in order to reasonably ensure the users' capital security, relevant departments and e-commerce enterprises should actively optimize the system security to effectively enhance resistance capability to virus invasion. At the same time, in response to malicious hacker attacks, relevant departments should actively improve relevant laws and regulations, and strengthen the punishment of personnel involved, so as to construct a safe network environment and provide guarantee for the reasonable solution of users' payment security issues. In addition, in order to further improve the security in the payment process, the propaganda and popularization of online payment knowledge should be carried out, thereby promoting and strengthening people's awareness of online payment security, and laying the foundation for the enhancement of payment security.

References

1. Hao L, Ma Y. Analysis of the current situation of electronic payment and information security in cross-border e-commerce in China (in Chinese). *China Logistics & Purchasing* 2019; (17): 46.
2. Zhang Y. Approaches and measures of transaction security and payment in e-commerce environment: Comments on "Security and Payment of EC" (in Chinese). *China Safety Science Journal* 2019; 29(4): 190.
3. Zhang H. Liabilities and rules for the damage of electronic payment services in e-commerce transactions (in Chinese). *Cognition and Practice* 2019; 37(2): 160. doi: CNKI:SUN:ZIYX.0.2019-02-036.
4. Yang L. Liabilities and rules for the damage of electronic payment services in e-commerce transactions. *Academic Journal of Zhongzhou* 2019; (2): 45-56. doi: 10.3969/j.issn.1003-0751.2019.02.009.
5. Cui D. Discussion on payment security under the integration of new media and e-commerce (in Chinese). *Today's Mass Media* 2017; 25(6): 18-19. doi: 10.3969/j.issn.1672-8122.2017.06.007
6. Liu L. Analysis and countermeasures of mobile payment security (in Chinese). *Internet Application* 2018; 20(22): 117. doi: CNKI:SUN:TXWL.0.2018-22-090
7. Chen Y. Issues and solutions of electronic payment security (in Chinese). *Modern Economic Information* 2018; (20): 306. doi: CNKI:SUN:XDJZ.0.2018-20-247.
8. Liu B. Analysis on the security and trust of Alipay (in Chinese). *Modern SOE Research* 2018; 146(20): 166. doi: CNKI:SUN:XDGQ.0.2018-20-143.
9. Fang Y. On the problems and solutions of electronic payment (in Chinese). *Modern Economic Information* 2018; (24): 305. doi: CNKI:SUN:XDJZ.0.2018-16-238.
10. Wang Y, Shen Y, Zhang X. Security issues and countermeasures of mobile payment under the background of

- "Internet +" (in Chinese). *Public Management* 2018; (22): 56-57. doi; CNKI:SUN:GLKW.0.2018-22-019.
11. Jing C. Mobile payment security issues and countermeasures of e-commerce platform in Wuwei City (in Chinese). *Computer Products and Circulation* 2018; (7): 126. doi: CNKI:SUN:WXXJ.0.2018-07-118.
 12. Wang L. Discussion on the security of NFC mobile payment (in Chinese). *Knowledge Economy* 2018; 464(11): 39-40. doi: 10.3969/j.issn.1007-3825.2018.11.023